

МИНОБРНАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ
Директор института прикладной
математики и компьютерных наук
А.В. Замятин
« 02 » Второй 2021 г.

Квантовые вычисления

рабочая программа дисциплины

Закреплена за кафедрой	<i>компьютерной безопасности</i>
Учебный план	<i>10.05.01 Компьютерная безопасность, профиль «Анализ безопасности компьютерных систем»</i>
Форма обучения	<i>очная</i>
Общая трудоёмкость	<i>4 з.е.</i>
Часов по учебному плану	<i>144</i>
в том числе:	
аудиторная контактная работа	<i>54,7</i>
самостоятельная работа	<i>89,3</i>
Вид(ы) контроля в семестрах	
экзамен/зачет/зачет с оценкой	<i>Семестр А – экзамен</i>

Программу составил:
канд. техн. наук,
доцент кафедры компьютерной безопасности



В.Н. Тренькаев

Рецензент:
канд. техн. наук,
заведующий кафедрой компьютерной безопасности



С.А.Останин

Рабочая программа дисциплины «Квантовые вычисления» разработана в соответствии с образовательным стандартом высшего образования – специалитет, самостоятельно устанавливаемым федеральным государственным автономным образовательным учреждением высшего образования «Национальный исследовательский Томский государственный университет» по специальности 10.05.01 Компьютерная безопасность (Утвержден Ученым советом НИ ТГУ, протокол от 30.06.2021 г. № 06).

Рабочая программа одобрена на заседании кафедры компьютерной безопасности

Протокол от 02 июня 2021 г. № 06

Заведующий кафедрой компьютерной безопасности,
канд. техн. наук, доцент



С.А. Останин

Рабочая программа одобрена на заседании учебно-методической комиссии института прикладной математики и компьютерных наук (УМК ИПМКН)

Протокол от 17 июня 2021 г. № 05

Председатель УМК ИПМКН,
д-р техн. наук, профессор



С.П. Сущенко

Цель освоения дисциплины – сформировать у студентов способность учитывать современные тенденции развития информационных технологий в своей профессиональной деятельности, в частности ознакомить с основами квантовых вычислений и квантовой криптографии.

1. Место дисциплины в структуре ОПОП

Дисциплина «Квантовые вычисления» относится к части, формируемой участниками образовательных отношений Блока 1 «Дисциплины».

Для освоения дисциплины необходимо знать основы физики, информатики, линейной алгебры, теории вероятностей, теории чисел, теории кодирования, дискретной математики, криптографии.

Пререквизиты дисциплины: Физика, Информатика, Общая алгебра, Дискретная математика, Теория чисел, Методы и средства криптографической защиты информации

Постреквизиты дисциплины: Производственная практика, Преддипломная практика

2. Компетенции и результаты обучения, формируемые в результате освоения дисциплины

Таблица 1.

Компетенция	Индикатор компетенции	Код и наименование результатов обучения (планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций)
ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ИОПК-1.1 Учитывает современные тенденции развития информационных технологий в своей профессиональной деятельности.	ОР-1.1.1 Знать: историю создания и основные характеристики квантового компьютера
ОПК-3. Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности	ИОПК-3.2 Осуществляет применение основных понятий, фактов, концепций, принципов математики и информатики для решения задач профессиональной деятельности.	ОР-3.2.1 Знать: математические основы квантовых вычислений и принципы работы квантового компьютера
ОПК-7. Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач,	ИОПК-7.3 Демонстрирует навыки создания программ с применением методов и инструментальных средств программирования для решения различных профессиональных, исследовательских и прикладных задач.	ОР-7.3.1 Уметь: применять требуемый математический аппарат для вычисления значений квантовых схем. ОР-7.3.2 Владеть: инструментальными средствами моделирования квантовых схем.

осуществлять обоснованный выбор инструментария программирования и способов организации программ		
ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации	ИОПК-9.1 Учитывает современные тенденции развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных при решении задач своей профессиональной деятельности.	ОР-9.1.1 Знать: основные квантовые алгоритмы, квантовые протоколы распределения ключей, квантовые протоколы передачи данных.
ПК-2. Способен разрабатывать требования к программно-аппаратным средствам защиты информации компьютерных систем и сетей	ИПК-2.2 Разрабатывает математические модели, реализуемые в средствах защиты информации. ИПК-2.3. Проводит исследования с целью нахождения наиболее целесообразных практических решений по обеспечению защиты информации	ОР-2.2.1 Уметь: излагать и демонстрировать на примерах квантовые алгоритмы и протоколы. ОР-2.2.2 Владеть: навыками анализа и синтеза квантовых схем.

3. Структура и содержание дисциплины

3.1. Структура и трудоемкость видов учебной работы по дисциплине

Общая трудоемкость дисциплины составляет 4 зачетные единицы, 144 часа.

Таблица 2.

Вид учебной работы	Трудоемкость в академических часах	
	Семестр А	всего
Общая трудоемкость	144	144
Контактная работа:	54,7	54,7
Лекции (Л):	32	32
Практики (ПЗ)		
Лабораторные работы (ЛР)	16	16
Семинары (СЗ)		
Групповые консультации	2	2
Индивидуальные консультации	2,4	2,4
Промежуточная аттестация	2,3	2,3
Самостоятельная работа обучающегося:	89,3	89,3
- подготовка к лабораторным занятиям	22	22
- изучение учебного материала, публикаций	35,6	35,6
- подготовка к рубежному контролю по теме/разделу	31,7	31,7
Вид промежуточной аттестации (зачет, зачет с оценкой, экзамен)	Экзамен	Экзамен

3.2. Содержание и трудоемкость разделов дисциплины

Таблица 3.

Код занятия	Наименование разделов и тем и их содержание	Вид учебной работы, занятий, контроля	С е м е с т р	Часы в электронной форме	Всего (час.)	Литература	Код (ы) результата(ов) обучения
	Раздел 1. Введение в квантовые вычисления		А		9	1,2,7	ОР-1.1.1
1.1.	Квантовая гонка.	Лекция	А		2		
1.2.	Квантовый компьютер.	Лекция	А		2		
1.3.	Квантовые вычисления.	СРС	А		5		
	Раздел 2. Математические основы квантовых вычислений		А		9	1,2,6	ОР-3.2.1
2.1.	Линейное пространство. Линейные операторы.	Лекция	А		2		
2.2.	Обратимые вычисления. Обратимые вентили.	Лекция	А		2		
2.3.	Обратимые схемы.	СРС	А		5		
	Раздел 3. Квантовые схемы		А		10	1-7	ОР-7.3.1, ОР-7.3.2, ОР-2.2.2
3.1.	Кубит. Одно/двух/трехкубитовые вентили.	Лекция	А		2		
3.2.	Простые квантовые схемы. Вычисление булевой функции.	Лекция	А		2		
3.3.	Квантовая схема Базис Белла.	ЛР	А		2		
3.4.	Квантовая схема Reverse CNOT.	ЛР	А		2		
3.5.	Квантовая схема SWAP.	ЛР	А		2		
3.6.	Сложные квантовые схемы.	СРС	А		7,6		
	Раздел 4. Квантовые протоколы		А		16	4,5	ОР-2.2.1, ОР-9.1.1
4.1.	Квантовые протоколы передачи данных.	Лекция	А		2		
4.2.	Квантовые протоколы распределения ключей.	Лекция	А		4		
4.3.	Квантовые протоколы. ЭПР-протокол.	СРС	А		10		
	Раздел 5. Квантовые алгоритмы		А		40	1-7	ОР-9.1.1, ОР-7.3.2, ОР-2.2.1, ОР-2.2.2
5.1.	Алгоритм Дойча – Джозса. Алгоритм Бернштейна – Вазирани	Лекция	А		2		
5.2.	Алгоритм Саймона. Алгоритм Гровера.	Лекция	А		2		
5.3.	Квантовое преобразование Фурье. Алгоритм Шора.	Лекция	А		6		
5.5.	Алгоритм Дойча	ЛР	А		2		
5.6.	Алгоритм Бернштейна – Вазирани	ЛР	А		4		

5.7.	Алгоритм Гровера	ЛР	А		4		
5.8.	Языки квантового программирования	СРС	А		20		
	Раздел 6. Квантовая коррекция ошибок		А		14	5	ОР-9.1.1
6.1.	Общая схема квантовых кодов.	Лекция	А		2		
6.2.	Трехкубитовый квантовый код.	Лекция	А		2		
6.3.	Алгоритмы QEC	СРС	А		10		
	Подготовка к промежуточной аттестации в форме экзамена	СРС	А		31,7	1-7	
	Прохождение промежуточной аттестации в форме экзамена	Э	А		4,3		

4. Образовательные технологии, учебно-методическое и информационное обеспечение для освоения дисциплины

Образовательная технология – посещение студентом последовательности из набора лекций по разным темам дисциплины с последующим выполнением лабораторных работ по пройденным темам. Самостоятельная работа студентов включает подготовку к лабораторным занятиям, изучение учебного материала и публикаций, подготовку к рубежному контролю по разделу. Учебно-методическое обеспечение включает: список основной и дополнительной учебной литературы, список информационных ресурсов в сети Интернет, базу данных статей по квантовым вычислениям, слайды лекционных занятий, методические рекомендации по выполнению лабораторных работ. Промежуточная аттестация осуществляется на основе выполнения лабораторных работ, а также по результатам собеседования с использованием перечня контрольных вопросов по курсу.

Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения, характеризующих этапы формирования компетенций, и методические материалы, определяющие процедуры оценивания результатов обучения, приведены в Приложении 1 к рабочей программе «Фонд оценочных средств».

Типовые контрольные задания или иные материалы, необходимые для текущей аттестации, и методические материалы, определяющие процедуры оценивания результатов текущей аттестации, приведены в Приложении 2 к рабочей программе «Примерные оценочные средства текущей аттестации».

4.1. Рекомендуемая литература и учебно-методическое обеспечение

№ п/п	Авторы / составители	Заглавие	Издательство	Год издания, количество страниц
Основная литература				
1.	Сысоев С. С.	Введение в квантовые вычисления. Квантовые алгоритмы : учебное пособие	СПб : Изд-во С.-Петербур. ун-та	2019 г., 144 с.
2.	Торгаев С.Н., Шульга И.Д., Юрченко Е.А., Громов М.Л.	Основы квантовых вычислений: учебное пособие.	Томск: STT	2020 г., 100 с.
3.	Райли Т. Перри	Элементарное введение в квантовые вычисления. Учебное пособие.	М.: ИНТЕЛЛЕКТ	2015 г., 203 с.
4.	Альбов А.С.	Квантовая криптография	Санкт-Петербург: СТРАТА	2015 г., 245 с.
Дополнительная литература				
5	Нильсен М., Чанг И.	Квантовые вычисления и квантовая информация	М.: Мир	2006 г., 824 с.
6.	Имре Ш., Баланж Ф.	Квантовые вычисления и связь. Инженерный подход	М.: ФИЗМАТЛИТ	2008 г, 320 с.
7.	Кайе Ф., Лафлам Р., Моска М.	Введение в квантовые вычисления	Ижевск: Регулярная и хаотическая динамика	2009 г., 360 с.

4.2. Базы данных и информационно-справочные системы, в том числе зарубежные

1. Электронная библиотека (репозиторий) ТГУ [Электронный ресурс] / Электронная библиотека (репозиторий) ТГУ: [сайт]. – [Томск, 2011–2016]. – URL: <http://vital.lib.tsu.ru/vital/access/manager/Index>

2. Михаил Вялый, Александр Шень Курс “ Классические и квантовые вычисления” [Электронный ресурс] // Национальный Открытый Университет "ИНТУИТ". URL: <http://www.intuit.ru/studies/courses/1057/136/info>

4.3. Перечень лицензионного и программного обеспечения

- Операционная система Windows/Linux
- Браузер Firefox/Яндекс

4.4. Оборудование и технические средства обучения

Для реализации дисциплины необходимы лекционная аудитория и аудитория для проведения лабораторных занятий. Специальные технические средства (проектор, компьютер, доступ к сети Интернет) требуются для демонстрации материала в рамках изучаемых разделов и проведения лабораторных работ. Вся основная и дополнительная литература, необходимая для самостоятельной работы и подготовки к экзамену, имеется в научной библиотеке ТГУ.

5. Методические указания обучающимся по освоению дисциплины

- целенаправленно, систематически и планомерно работать со слайдами лекций;
- изучать рекомендуемую литературу, добывая новые/обобщая полученные знания;
- тратить не менее часа в день на самостоятельную работу;
- консультироваться с преподавателем при возникновении вопросов;
- активно использовать учебно-методический комплекс на базе Moodle ТГУ;
- работать с тематическими форумами в сети Интернет.

6. Преподавательский состав, реализующий дисциплину

Тренькаев Вадим Николаевич, канд. техн. наук, доцент, доцент кафедры компьютерной безопасности

7. Язык преподавания – русский язык.